ABSTRACT

Provided is a method for updating a group key in a highly secure manner and at high speed. A method includes: a step of making subscriber terminals (20) perform a part of decryption of an encrypted group key used to decrypt the information before distribution of the group key; a step of distributing the group key and individual decryption information used to perform a part of remaining decryption other than the part of decryption of the group key and corresponding to terminal devices to the subscriber terminals (20); and a step of making the subscriber terminals (20) perform decryption of the group key using the decryption information being distributed and results obtained by implementing a part of decryption of the group key, the part of decryption previously being performed.